

Barry University

PO Box 6336
Portland, OR 97228-6336

<<mail id>>
<<Name1>>
<<Name2>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>
<<Foreign Country>>

**IMPORTANT INFORMATION
PLEASE READ CAREFULLY**

<<Date>>

Dear FirstName LastName:

I am writing to you about a security incident that may have involved your personal information that is maintained by Barry University.

On May 14, 2013, Barry University detected the presence of a form of malware which infected a Barry University laptop computer and the files contained within it. Barry University immediately commenced an investigation of the incident and retained a third-party computer forensic company to investigate the extent of the infection, including identification, isolation and removal of the malware infection from Barry University's network. The affected files have been restored to their original state and there is no longer any evidence of active malware on the device.

Since completing the forensic investigation, we have devoted considerable time and effort to determine what exact information may have been on the affected device. We can confirm that the laptop contained your full name and one or more of the following: date of birth, Social Security number, driver's license number, and/or bank account number.

To date, we are not aware of any reports of identity fraud, theft, or other harmful activity resulting from this incident. Due to the complexity of the malware infection, however, Barry University cannot conclusively determine whether the malware was able to expose any of your personal information or whether an unauthorized person acquired your information. Out of an abundance of caution, we wanted to make you aware of this incident and explain the services we are making available to safeguard you against identity fraud. Please see the enclosed information.

Barry University takes this situation very seriously. We deeply regret that your personal information may have been exposed as a result of this incident. Maintaining the integrity of your confidential information is of the utmost importance to us. Enclosed you will find information on enrolling in a complimentary 12-month credit monitoring service along with other precautionary measures you can take to protect your personal information.

If you have any further questions regarding this incident, please call our toll-free number we have set up to respond to questions at 1-800-981-7571. When calling, please use reference number: 47911. The call center is available Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time.

Sincerely,



Yvette Brown
Chief Information Officer
Barry University

1. **Enrolling in Complimentary 12 Month Credit Monitoring**

Protecting your personal information is important to Barry University. In response to this security incident and as a precautionary measure, we have arranged for you to enroll in Experian's® ProtectMyID® Alert for a one year period at no cost to you. This protection is provided by Experian, one of the three major nationwide credit reporting companies.

Activate ProtectMyID Now in Three Easy Steps

1. ENROLL by **March 31, 2014**.
2. ENROLL at ProtectMyID Web Site, **www.protectmyid.com/redeem** OR **877-371-7902**
3. PROVIDE your 9-character Activation Code: XXXXXXXXXX

Once your ProtectMyID membership is activated, your credit report will be monitored daily for 50 leading indicators of identity theft. You'll receive timely Credit Alerts from ProtectMyID on any key changes in your credit report which could include new inquiries, new credit accounts, medical collections and changes to public records.

ProtectMyID provides you with powerful identity protection that will help detect, protect and resolve potential identity theft. In the case that identity theft is detected, ProtectMyID will assign a dedicated U.S.-based Identity Theft Resolution Agent who will walk you through the process of fraud resolution from start to finish for seamless service.

We realize that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.

Your complimentary 12-month ProtectMyID membership includes:

- **Credit Report:** A free copy of your Experian credit report
- **Daily 3 Bureau Credit Monitoring:** Alerts you of suspicious activity including new inquiries, newly opened accounts, delinquencies, or medical collections found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution:** If you have been a victim of identity theft, you will be assigned a dedicated, U.S.-based Experian Identity Theft Resolution Agent who will walk you through the fraud resolution process, from start to finish.
- **ExtendCARE:** Full access to the same personalized assistance from a highly-trained Fraud Resolution Agent even after your initial ProtectMyID membership expires.
- **\$1 Million Identity Theft Insurance:** As a ProtectMyID member, you are immediately covered by a \$1 Million insurance policy that can help you cover certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers. (Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of Chartis, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.)

If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-371-7902.

2. Placing a Fraud Alert

Whether or not you choose to use the complimentary 12 month credit monitoring services, we recommend that you place an initial 90-day "Fraud Alert" on your credit files. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

TransUnion

Consumer Fraud Division
PO Box 6790
Fullerton, CA 92834-6790
www.transunion.com/fraud
1-800-680-7289

Experian

Consumer Fraud Division
PO Box 9554
Allen, TX 75013
www.experian.com
1-888-397-3742

Equifax

Consumer Fraud Division
PO Box 740256
Atlanta, GA 30374-0256
www.equifax.com
1-800-525-6285

3. Obtaining a Free Credit Report

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit report online at **www.annualcreditreport.com**.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338) or by mail at 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations.

4. Contacting Your Banking Institution

If your banking information was involved in this incident, we advise you to call your banking institution to determine if you should change your bank account number.